

# Implementing Cisco SD-WAN Solutions (300-415)

*Memory Exercises Created by Luke Snell*



## Licensing and Right to Use Information

**Do not remove this section without the written permission of the author.**

This document is licensed under the Creative Commons Attribution Share Alike 4.0 International licence. You may freely use, modify and share this document provided that it is not resold for commercial gain. If you would like to rebrand and/or sell this document commercially then an exception request must be submitted and authorised (potentially requiring payment) from the author Luke Snell via [admin@ether-net.com](mailto:admin@ether-net.com),

Cisco SD-WAN and Viptela remains the property of Cisco Systems Inc and/or its affiliates.

## Document Information

<b>Document Title</b>	Implementing Cisco SD-WAN Solutions (300-415): Memory Exercises
<b>Brief Description</b>	A document to assist persons studying for the CCNP Enterprise specialist exam "Implementing Cisco SD-WAN Solutions (300-415)"
<b>Create Date</b>	30.08.20
<b>Author</b>	Luke Snell
<b>Version</b>	1.0

## Revision History

<b>Date</b>	<b>Version</b>	<b>Revised by</b>	<b>Revision Notes</b>
23.11.20	1.0	Luke Snell	Initial Public Release

## How to Use this Document

**This document has been created for people that are preparing to sit the CCNP Enterprise specialist exam “*Implementing Cisco SD-WAN Solutions (300-415)*”. It contains a variety of “memory exercises” that you can utilise during your studies to prepare for the official certification exam. These exercises have been derived from materials that I used while preparing for the exam.**

I firmly believe that familiarity with CLI syntax, the vManage GUI, and the Cisco SD-WAN API should be obtained through exposure to the technologies in a lab environment. So, with the exception of a handful of topics, no memory exercises contain command syntax or configuration “how to’s”. **I have provided links to free and official Cisco resources that you can use to develop these skills if you do not have access to Cisco SD-WAN software.**

To get the most out of this document you should scan through it and identify topics whose “details” you do not feel confident recalling under exam conditions. The first page of every “topic” details the answers and is followed by templates you can use to print out and complete.

Proceed to printing off a suitable number of each exercise to complete only once you have identified your strengths and weaknesses! Your weakest topics should have more exercises to complete so that you do not waste time revising topics you are already comfortable with. Try to use the concept of [spaced repetition](#) to optimize your exam revision preparation.

With the exception of two topics – no memory exercises contain command syntax or configuration processes. Familiarity with CLI syntax, APIs, and the vManage GUI should all be developing via practical lab exercises. **You will need to know your show commands for the device administration section of this exam!**

Finally, please note that this is one of *many* resources you should utilise when preparing for the certification exam. This resource should help you avoid losing easy points in the 50 or so questions that will be thrown at you in the exam, however without labbing each topic thoroughly it will be difficult to crack the more complex exam questions.

Best of luck with your Cisco SD-WAN journey!

- Luke Snell

## Table of Contents

Table of Contents .....	4
ZTP Workflow .....	7
Cisco PnP Workflow.....	12
Colours & Public/Private IPs .....	14
NAT Types.....	16
OMP Route Table Abbreviations.....	18
OMP Route Attributes .....	20
TLOC Route Attributes.....	22
Service Route Attributes.....	24
OMP Best Path Selection.....	26
Policy Types .....	28
Policy Lists.....	30
Policy Application & Enforcement.....	32
Packet Forwarding Order of Operations .....	34
vManage NMS Services & Local Clustering.....	36
SD-WAN Syslog.....	39
Application Aware Routing.....	41
Quality of Service [QoS] .....	43
REST API Monitoring .....	46

## Cisco SD-WAN Hardware

It is a good idea to understand device feature capabilities [e.g.: WLAN / LTE built in] and what deployment scenario the devices are best used for. You should refer to hardware data sheets and design documentation for this information.

Use this memory table just to understand the hardware models associated with each software chain.

Viptela OS	Cisco IOS-XE
vEdge Cloud	Catalyst 8000V Edge, CSR1000v
vEdge-100/100b/100m	ASR 1001-X / 1002-X
vEdge-1000	Catalyst 8300 / 8500 Series
vEdge-2000	ISR 1000 Series [excl. ISR1100-4G/6G/LTE]
vEdge-5000	ISR 4000 Series
ISR 1100-4G/6G/LTE	ENCS 5000
	IR-1100 [industrial router]

## **Cisco SD-WAN Hardware**

Viptela OS	Cisco IOS-XE

Viptela OS	Cisco IOS-XE

Viptela OS	Cisco IOS-XE

## ZTP Workflow

### ZTP Workflow

#### 1. Confirm Pre-Requisites

- vManage has been configured and all certificates have been deployed
- Control connections established between controllers
- Full reachability to target site where vEdge is being deployed
- vBond IP is reachable across the enterprise
- vManage WAN Edge List is populated and the desired vEdge entry has been flagged as “staging” or “valid”

#### 2. Deploy second vBond and configure it to act as a ZTP-server, ensure its IP address is publicly reachable across the enterprise.

```
vbond <IP address of the ZTP server's transport interface> local ztp-server
```

#### 3. Configure enterprise DNS servers to resolve `ztp.viptela.com` to the vBond ZTP Server's transport interface IP[s]

#### 4. Create the ZTP chassis CSV or JSON [20.3.1+] file to following information:

- `chassis_number`
- `serial_or_token_number`
- `validity`: either invalid, staging or valid
- `vBond_IP`:
- [optional] `vBond_Port`
- `organization_name`
- [optional] `path_to_enterpriseCA`

## ZTP Workflow

5. Upload the ZTP chassis file with the command:

```
request device-upload chassis-file <location>
```

6. Verify the file entries were accepted and are valid:

```
show vtp entries
```

7. In vManage create a template for the vEdge device and attach it to its chassis/serial or chassis/token

8. [Optional] To enable ZTP Software Enforcement:

- Go to Maintenance > Software Repository and upload Cisco SD-WAN images
- Go to Administration > Settings and enable “Enforce Software Version [ZTP]”, select which nodes you want to enforce image management on and then select the required image version

9. Power on the vEdge device at the target site & allow time for ZTP process

**For enterprise managed certificate deployments the Root CA cert must be installed on vEdge and it must be preconfigured with** `system organization-name <ORG_NAME>`

**For vEdge-cloud devices, must use command** `activate vedge-cloud chassis-number <chassis_num> token <token>` **to start the ZTP process**

**If ZTP Software enforcement was enabled its transfer progress can be monitored via vManage Tasks**

10. Verify vEdge device configuration aligns with device template and whether it is running the correct image version [if configured in Step 8]



## **ZTP Workflow**

*Only write down core concepts for each step*

### **ZTP Workflow – Page 1**

1. Pre-requisites:

- 
- 
- 
- 
- 

2.

3.

## ZTP Workflow – Page 2

4.

---

- ---
- ---
- ---
- ---
- ---
- ---

5.

6.

## ZTP Workflow – Page 3

7.

8.

- \_\_\_\_\_
- \_\_\_\_\_  
\_\_\_\_\_

9.

10.

## Cisco PnP Workflow

Step	Action
1	vManage has a device template preconfigured
2	Node boots up and obtains DHCP IP/DNS/Default Gateway information on transport interface
3	Node queries devicehelper.cisco.com
4	Cisco PnP SaaS Service redirects to corporate vBond
5	vBond initiates control communication
6	Node receives vManage device template

## **Cisco PnP Workflow**

Step	Action
1	
2	
3	
4	
5	
6	

Step	Action
1	
2	
3	
4	
5	
6	

## Colours & Public/Private IPs

**Private Colours:** used where no NAT addressing of transport IP endpoints occurs

metro-ethernet	mpls	private1 – private6
----------------	------	---------------------

**Public Colours:** used where NAT addressing of transport IP endpoints occurs

3g	biz-internet	lte	public-internet
blue/bronze/green/red/gold	custom1-3		

**Private IP:** Any IP address assigned to interface, pre-NAT address

**Public IP:** Same as “private IP” if no NAT, else it’s post-NAT address

Source Colour Type	Destination Colour Type	IPs used...	
Public	Public	Public	Private
Public	Private	Public	Private
Private	Private	Public	Private

## Colours and Public/Private IPs

**Private Colours:** \_\_\_\_\_

--	--	--

**Public Colours:** \_\_\_\_\_


**Public IP:** \_\_\_\_\_

**Private IP:** \_\_\_\_\_

Source Colour Type	Destination Colour Type	IPs used...	
Public	Public	Public	Private
Public	Private	Public	Private
Private	Private	Public	Private

## NAT Types

Type	Comment
Full Cone / One-to-One NAT	Maps internal address/port pair to external address/port pair.
Address-Restricted Cone NAT [Restricted Cone NAT]	Permits outbound connections inwards IF-AND-ONLY-IF a session was established from the inside first.
Port Restricted Cone NAT	Stricter version of Restricted Cone NAT where ports are added to process.
Symmetric NAT	<p>Unique external IP/port mapping created for each destination IP/port.</p> <p>Outbound connections permitted inwards only if inside network initiated stream.</p> <p>Only supported on one end of the tunnel and with One-to-One NAT.</p>

wEdge A	wEdge B	IPSec Tunnel Formed?	
Public IP [No Nat]	Public IP [No Nat]	Yes	No
Full Cone	Full Cone	Yes	No
Full Cone	Address/Port Restricted NAT	Yes	No
Address/Port Restricted NAT	Address/Port Restricted NAT	Yes	No
Public	Symmetric	Yes	No
Full Cone	Symmetric	Yes	No
Symmetric	Address/Port Restricted NAT	Yes	No
Symmetric	Symmetric	Yes	No



## NAT Types

Type	Comment
Full Cone / One-to-One NAT	
Address-Restricted Cone NAT [Restricted Cone NAT]	
Port Restricted Cone NAT	
Symmetric NAT	<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> </ul>

wEdge A	wEdge B	IPSec Tunnel Formed?	
Public IP [No Nat]	Public IP [No Nat]	Yes	No
Full Cone	Full Cone	Yes	No
Full Cone	Address/Port Restricted NAT	Yes	No
Address/Port Restricted NAT	Address/Port Restricted NAT	Yes	No
Public	Symmetric	Yes	No
Full Cone	Symmetric	Yes	No
Symmetric	Address/Port Restricted NAT	Yes	No
Symmetric	Symmetric	Yes	No

## OMP Route Table Abbreviations

Symbol	Meaning
C	Chosen
I	Installed
Red	Redistributed
Rej	Rejected
L	Looped
R	Resolved
S	Stale
Ext	Extranet
Inv	Invalid
Stg	Staged
U	TLOC Unresolved

## OMP Route Table Abbreviations

Symbol	Meaning	Symbol	Meaning
C		U	
I		Stg	
Red		Inv	
Rej		Ext	
L		S	
R		R	
S		L	
Ext		Rej	
Inv		Red	
Stg		I	
U		C	

Symbol	Meaning	Symbol	Meaning
C		U	
I		Stg	
Red		Inv	
Rej		Ext	
L		S	
R		R	
S		L	
Ext		Rej	
Inv		Red	
Stg		I	
U		C	

## OMP Route Attributes

Attribute	Description
TLOC	Next-hop of the OMP route
Origin	Source of the route and may contain a protocol identifier Used for best path selection
Originator	System IP of advertiser – details where route learnt from
Preference	Higher = Better ; influences best path selection process
Service	Indicates the service this route is tied to [if any]
Site ID	Should be unique per site, used for loop prevention
Tag	Route Tag, transitive attribute not carried across redistribution
VPN	The VPN/VRF route was advertised FROM
AD	<i>Not an OMP Attribute but RIB AD is...:</i> <ul style="list-style-type: none"><li>• Viptela: 250</li><li>• IOS-XE: 251</li></ul>

[illegible]

## TLOC Route Attributes

Attribute	Description
TLOC Private Address	Contains private IP address of the wEdge interface
TLOC Public Address	STUN used to notify wEdge if behind NAT - will represent post NAT address in this case. If same as private address then wEdge not behind NAT.
Color	Color of transport
Encapsulation Type	GRE or IPSec, must match on both sides of tunnel
Preference	Higher = Better, used for path selection
Site ID	Identifies originator & used with IPSec tunnel construction
Tag	Route tag
Weight	Higher = Better, used for path selection, locally significant

### TLOC Route Attributes

[illegible][illegible]

## Service Route Attributes

Attribute	Description
VPN ID	VPN service belongs to
Service ID	Identifies service type being advertised: <ul style="list-style-type: none"><li>• <b>FW:</b> Firewall [svc-id1]</li><li>• <b>IDS:</b> Intrusion Detection System [svc-id2]</li><li>• <b>IDP:</b> Identity Provider [svc-id3]</li><li>• <b>netsvc1-4:</b> custom, maps to svc-id 4-7 respectively</li></ul>
Label	Substitute label for OMP routes who must be redirected to the service
Originator ID	System IP address of advertising node
TLOC	Identifies where the service is located
Path ID	Identifies the OMP Path



## Service Route Attributes

Attribute	Description
	<ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>•</li></ul>

Attribute	Description
	<ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>•</li></ul>

## OMP Best Path Selection

Step	Operation
1	Confirm OMP route is valid
2	Prefer locally sourced OMP routes to vSmart sourced OMP routes
3	Prefer lower AD routes
4	Prefer higher OMP preference
5	Prefer higher TLOC preference
6	Prefer the origin whose default AD is lower [e.g.: Static beats iBGP]
7	Prefer lowest Origin metric
8	Prefer highest System IP
9	Prefer highest TLOC private address

## **OMP Best Path Selection**

Step	Operation
1	
2	
3	
4	
5	
6	
7	
8	
9	

Step	Operation
1	
2	
3	
4	
5	
6	
7	
8	
9	

## Policy Types

Central Control	Central Data
Control	Traffic Data
VPN Membership	Application Aware Routing
	Cflowd

Traditional Localised Policy	Security Policy
Route Policy	Firewall
QoS	Intrusion Prevention
ACLs	URL Filtering
	AMP
	DNS Security

## **Policy Types**

Central Control	Central Data

Traditional Localised Policy	Security Policy

Central Control	Central Data

Traditional Localised Policy	Security Policy

Central Control	Central Data

## Policy Lists

Name	Purpose
Application	Match on an application / app family
Colour	Specify a single colour or colour group
Prefix	Match routing info in control plane specifically
Data Prefix	Match data in the data plane specifically
Site	Matching criteria to determine where policy application occurs
Policers	Limit ingress/egress traffic, cannot match off
SLA Class	Defines loss, latency and jitter that a class of traffic experience
TLOC	Used to manipulate next-hop of traffic forwarded
VPN	Service-side VPNs for which data policy should be applied to

## Policy Lists

[illegible][illegible]

## Policy Application & Enforcement

	Applied To...		Enforced On...	
Data Policy	vSmart	wEdge	vSmart	wEdge
App-Aware Routing Policy	vSmart	wEdge	vSmart	wEdge
Control Policy	vSmart	wEdge	vSmart	wEdge
VPN Membership Policy	vSmart	wEdge	vSmart	wEdge
Localized Policy	vSmart	wEdge	vSmart	<b>wEdge</b>
Security Policy	vSmart	wEdge	vSmart	<b>wEdge</b>
cFlowd	vSmart	wEdge	vSmart	<b>wEdge</b>



## **Policy Application & Enforcement**

	Applied To...		Enforced On...	
Data Policy	vSmart	wEdge	vSmart	wEdge
App-Aware Routing Policy	vSmart	wEdge	vSmart	wEdge
Control Policy	vSmart	wEdge	vSmart	wEdge
VPN Membership Policy	vSmart	wEdge	vSmart	wEdge
Localized Policy	vSmart	wEdge	vSmart	wEdge
Security Policy	vSmart	wEdge	vSmart	wEdge
cFlowd	vSmart	wEdge	vSmart	wEdge

	Applied To...		Enforced On...	
Data Policy	vSmart	wEdge	vSmart	wEdge
App-Aware Routing Policy	vSmart	wEdge	vSmart	wEdge
Control Policy	vSmart	wEdge	vSmart	wEdge
VPN Membership Policy	vSmart	wEdge	vSmart	wEdge
Localized Policy	vSmart	wEdge	vSmart	wEdge
Security Policy	vSmart	wEdge	vSmart	wEdge
cFlowd	vSmart	wEdge	vSmart	wEdge

	Applied To...		Enforced On...	
Data Policy	vSmart	wEdge	vSmart	wEdge
App-Aware Routing Policy	vSmart	wEdge	vSmart	wEdge
Control Policy	vSmart	wEdge	vSmart	wEdge
VPN Membership Policy	vSmart	wEdge	vSmart	wEdge
Localized Policy	vSmart	wEdge	vSmart	wEdge
Security Policy	vSmart	wEdge	vSmart	wEdge

## Packet Forwarding Order of Operations

Step	Operation
1	IP Destination Lookup
2	Ingress Interface ACL <i>If denied then drop packet</i>
3	Application-Aware Routing <i>Requires equal cost multipath (ECMP) routes in routing table</i>
4	Centralized Data Policy <i>Can override Step 3 decision</i>
5	Routing and Forwarding
6	Security Policy <i>Firewall &gt; Intrusion Prevention &gt; URL-Filtering &gt; AMP</i>
7	Encapsulation and Encryption
8	Egress Interface ACLs <i>Changes occur prior to packet forwarding</i>

Implementing Cisco SD-WAN Solutions (300-415) Memory Exercises  
by Luke Snell from <https://ether-net.com>

Step	Operation
1	
2	
3	
4	
5	
6	
7	
8	

Step	Operation
1	
2	
3	
4	
5	
6	
7	
8	

## vManage NMS Services & Local Clustering

Server / Service	Used For
Application Server	Web GUI, APIs – uses Wildfly
Statistics Database	Elasticsearch database for stats, audit logs, alarms, and events
Configuration Database	Stores config info, policies, templates, certificates.
Messaging Server	Kafka server that exchanges messages between vManage devices in a cluster
SD-AVC	“Software Defined Application Visibility and Control”  Optional service

### Greenfield Clustering Process

1. Plan for 3x vManage deployment – odd number required for quorum
2. Reserve & allocate 1G/10G interface on host for vManage cluster comms
3. Configure cluster interface in VPN 0 with an IP and no tunnel-interface
4. Configure “primary” node administration settings + certificates
5. Add “primary” node to the cluster in Administration > Cluster Configuration by adding its cluster interface IP and specifying admin credentials
6. Wait for cluster configuration process to complete, be patient.  
  
**Monitor NMS Service Restart:** `request nms all status`  
**Monitor via vShell:** `show log vmanage-server.log tail N`
7. Repeat steps 5 & 6 for subsequent cluster nodes
8. Once all nodes have joined the cluster onboard them as controllers via the primary node by generating CSR & installing their signed certificate.

## **vManage NMS Service & Clustering**

Server / Service	Used For
Application Server	
Statistics Database	
Configuration Database	
Messaging Server	
SD-AVC	

## Greenfield Clustering Process

1.

2.

3.

4.

5.

6.

7.

8.

## SD-WAN Syslog

File Name	Used For
auth.log	login, logout, superuser access events, usage of authorization systems
kern.log	kernel messages
messages	Consolidated log file containing syslog from all sources
vconfd	Configuration logging
vdebug	Storing running debugs – cannot be remotely sent
vsyslog	Viptela daemons

## **SD-WAN Syslog**

File Name	Used For

File Name	Used For



## Application Aware Routing

AAR Component	Use
Hello Interval	Frequency Hello is sent across a tunnel, default 1000 ms
Hello Multiplier	Number of BFD Hellos lost before declaring tunnel down, default 7
App-Route Poll Interval	Period of time used to calculate loss, latency and jitter from BFD Also known as “buckets” Be careful with config else results may not be statistically significant
App-Route Multiplier	Determines circuit health by evaluating results from App-Route Poll Intervals, default is 6 buckets

Step	Configuration Action
1	Define SLA Parameters
2	Define Application Lists
3	Define Sites, Prefixes and VPNs
4	Define the AAR Policy
5	Apply AAR Policy to Selected Sites

Scenario	Result
No tunnels match SLA	Distribute traffic among compliant tunnels
Single tunnel matches SLA	Send traffic through the compliant tunnel
Multiple tunnels match SLA	Revert to backup-sla-preferred-color if configured Last resort - send traffic through any available transport
<b>AAR requires at least 2 equal cost routes installed in the routing table to work!</b> <b>Max 4 SLA classes per vEdge</b>	

## Application Aware Routing

AAR Component	Use

Step	Configuration Action
1	
2	
3	
4	
5	

Scenario	Result

## Quality of Service [QoS]

Action	Comment
Classification	
Policing	
Scheduling	
Rewriting	

QoS Policy	Notes
Centralized Data	<ul style="list-style-type: none"><li>▪ Outbound direction = Service Class VPN to WAN</li><li>▪ Inbound Direction = WAN to Service Class VPN</li><li>▪ Enables QoS at a site level and supports DPI</li></ul>
Localized Data	<ul style="list-style-type: none"><li>▪ Outbound direction = Service Class VPN to WAN</li><li>▪ Inbound Direction = WAN to Service Class VPN</li><li>▪ Enables QoS at a site level and supports DPI</li></ul>

Step	Action
1	Define groups of interest: <ul style="list-style-type: none"><li>• Class Map</li><li>• [Optional] Policer to either drop or remark</li></ul>
2	Create QoS Map by linking Class Map to Queues, specify bandwidth/buffer
3	[Optional] Create QoS Rewrite Policy
4	Create ACLs to match traffic and classify / police traffic

## **QoS Treatment on wEdges – Part 1**

Action	Comment
Classification	
Policing	
Scheduling	
Rewriting	

QoS Policy	Notes
Centralized Data	<ul style="list-style-type: none"><li>▪</li><li>▪</li><li>▪</li></ul>
Localized Data	<ul style="list-style-type: none"><li>▪</li><li>▪</li><li>▪</li></ul>

## QoS Treatment on wEdges – Part 2

Step	Action
1	<ul style="list-style-type: none"><li>•</li><li>•</li></ul>
2	
3	
4	

Step	Action
1	<ul style="list-style-type: none"><li>•</li><li>•</li></ul>
2	
3	
4	

## REST API Monitoring

HTTP Method	Action
GET	Retrieves an object
POST	Creates an object, requires JSON body
PUT	Updates an object, requires JSON body
DELETE	Deletes an object

### Using the SD-WAN REST API

#### 1. Identify what you want to monitor

- vManage
  - Alarms Details, Events, Server Info
- SD-WAN devices
  - Device Details, Device Statistics Details, Interface Statistics
- Security
  - ipsalert, Umbrella, Umbrella Patterns, URL Filtering
- Traffic
  - Application-Aware Routing, cFlowd Flows, DPI, Flow Log, QoS

#### 2. Review relevant API docs via `https://<vmanage>/apidocs`

#### 3. Authenticate to vManage via `https://<vManage>/j_security_check`

- **Header:** `Content-Type : application/x-www-form-urlencoded`
- **Body:** `j_username , j_password`

#### 4. Make appropriate calls to retrieve data

## **REST API Monitoring**

HTTP Method	Action
GET	
POST	
PUT	
DELETE	

HTTP Method	Action
GET	
POST	
PUT	
DELETE	

HTTP Method	Action
GET	
POST	
PUT	
DELETE	

HTTP Method	Action
GET	
POST	
PUT	
DELETE	

## Using the SD-WAN REST API

1. \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

2.

3.

4.